

Chapter Name

7.0 Privacy

Chapter Number Title

7.2 Data Classification

1.0 Purpose

While Eastern Michigan University (EMU) information may reside in paper format, in different database management systems, or on different machines, these data, in the aggregate, may be thought of as forming a single, logical database. These data will be called institutional (or proprietary) data. This policy will describe the roles and responsibilities of EMU Employees, EMU affiliates, Functional Security Representatives (FSR) for Enterprise Resource Planning (ERP) systems and Data Stewards for other institutional data, and the procedures for establishing appropriate access and controls.

All institutional data should be used with appropriate and relevant levels of access and with sufficient assurance of its security and integrity in compliance with existing laws, rules, and regulations.

2.0 Scope

This section applies to institutional data only, as defined above, and is intended to provide appropriate access to these data by employees and affiliates for conducting institutional business. In all cases, applicable statutes, rules, and regulations that guarantee either protection or accessibility of institutional records will take precedence over this section. While this policy is especially pertinent to information stored electronically, it is applicable to all information, such as paper, microform, and video, as well as the content of confidential meetings and conversations.

This policy does not apply to notes and records that are the personal property of individuals in the institutional community.

The scope of this policy is to have broad application, particularly with respect to data and information resources, which have impact on institutional operation. Data that may be managed locally may also have significant impact if it is used in a manner that can impact institutional operations. It is expected that the intent of this section be extended in analogous manner to all data and information used at all operational levels of the institutional.

3.0 Policy

By default, all institutional data will be designated for internal use only or as to satisfy institutional external reporting requirements to the EMU Board of Regents (BOR), and to State, Federal, or other external agencies. EMU employees and affiliates will have access to these data for use in the conduct of institutional business. These data, while available within EMU, are not designated as open to the general public unless otherwise required by law. The permission to view or query institutional data should be granted to all data users for all legitimate institutional purposes. The EMU Office of Legal Affairs shall be consulted before outside release, when appropriate.

The FSR or data steward of systems that do not have a FSR assigned are responsible for identifying and classifying data associated with the confidential classification only when used in conjunction with personally identifiable information and

provide samples of the other two categories of data. With this approach, not every field will be assigned a classification. Refer to [The EMU Data Classification Matrix](#).

In some circumstances, as long as specific identifying data elements are removed, a data view may include elements of institutional data that would otherwise be sensitive or confidential.

All EMU information is categorized into three main classifications:

Public Data - institutional data that have no access restrictions and is available to both EMU affiliates and the general public. Additionally, statistical data in aggregate form that meets the [National Center for Education Statistics \(NCES\) Standard](#) . (Example: Information on the Universities public web site or data provided by Institutional Reporting and Information Management IRIM).

Sensitive Data - institutional data for which users must be granted specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the institution. Non-public or Internal data is moderately sensitive in nature, Often, this data is used for making decisions and therefore it is important this information remain timely and accurate.

Confidential Data - institutional data for which the highest levels of restriction should apply due to the risk or harm that may result from disclosure or inappropriate use (data protected by state and federal regulations such as FERPA, HIPAA & GLBA). Confidential data may have personal privacy considerations, only those individuals designated with approved access and signed non-disclosure agreements may be granted access to this data.

For internal use when in doubt about the classification, an EMU employee or affiliates shall:

- Contact their supervisor for guidance and verification,
- Contact the module specific FSR (<https://it.emich.edu/security/itso.cfm>),
- Contact the Director of IT Security (<https://it.emich.edu/security/itso.cfm>), or
- Escalate the classification to the next higher level for immediate handling of the data until clarification may be obtained.

4.0 Responsibility for Implementation

Functional Security Representatives and the Director of IT Security are responsible for the implementation of this policy. The Director of IT Security shall cause the Data Classification Matrix to be maintained and amended from time to time as deemed necessary due to changing conditions affecting data security, subject to final approval of the CIO of the University.,.

5.0 Enforcement

Enforcement will be handled by the Director of IT Security Administration and Director IT, Network and Systems.

Any employee found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under University policy. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including discharge.
- Criminal prosecution.

Any student found to violate federal or state of Michigan laws, EMU policies, procedures or standards of conduct, will be subject to disciplinary action under EMU's Student Code of Conduct. Any suspected violation of State or Federal laws will be reported to the appropriate legal authority for investigation.

Consequences for violations (in no particular order) include, but are not limited to:

- Verbal warnings.
- Revocation of access privileges.
- Disciplinary actions up to and including suspension or expulsion from school.
- Criminal prosecution.

If you break the law, you can be prosecuted. Even if you are not charged criminally, you can be held personally liable, and you can be suspended or dismissed from the University, or fired if you are an employee.

The University reserves the right to protect its electronic resources from threats of immediate harm. This may include activities such as disconnecting an offending computer system from the campus network, terminating a running job on a computer system, or taking other action.

6.0 Definitions	
<u>Term</u>	<u>Definition</u>
Functional Security Representatives	An FSR administers and approves access to data contained within a specific module within the Enterprise Resource Planning (ERP) system. They can be employees of University divisions other than Information Technology .
Enterprise Resource Planning (ERP) System	The management information systems (MISs) that integrate and automate many of the business practices associated with the operations or production of the University.
Data Stewards	EMU employees administering access control to EMU systems that are external to the ERP system
Institutional (proprietary) data	EMU data needed for the operation of the institution and the required data collected for students past and present, employees past and present, and external companies with which we do business.
Logical database	Information stored on multiple media, in different formats, and/or machines that comprise EMU's base of information. This includes but not limited to: financial, student, payroll, donor, health center, and ID system.
Data Classification Matrix	This is a table of data types and their security classification for Eastern Michigan University. It can be found at: http://

7.0 Revision History			
<u>Creator</u>	<u>Description</u>	<u>Submission Date</u>	<u>Approval Date</u>
Dorendorf	Initial draft based on SAN's policy template and Medical College of Georgia policies		
Dorendorf	FSR Meeting Comments	March 12, 2007	
Barr, Arnold	Added definition of Data Classification Matrix, some minor editorial changes, and added delegation of authority to Director of IT Security to maintain the Data Classification Matrix.	December 5, 2007	
Dorendorf	Final review of Policy Committee	November 18, 2008	
Dorendorf	Sent to Legal for Comments	November 25, 2008	
Dorendorf, Barkoff, Barr	Reviewed with Office of Legal Affairs	January 15, 2009	

Barr	<p>Modified last sentence, first paragraph, Section 3.0 as suggested by Office of Legal Affairs – Town Hall is next step. Run final spell check.</p> <p>Note: Finalize 7.2 Data Classification Matrix, then upload to IT Policy pages on Web server. Then create link to the Data Classification Matrix in second paragraph of Section 3.0.</p>	January 16, 2009	
Barr	Modified 5.0 Enforcement to include expanded clause	February 24, 2009	